IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,	)	
	)	
Plaintiff,	)	
	)	Civil Action No. 1:23-cv-09518-PAE-BCM
v.	)	
	)	
SOLARWINDS CORP. and TIMOTHY G. BROWN,	)	
	)	
Defendants.	)	

DECLARATION OF RANI JOHNSON IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Rani Johnson, hereby declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, as follows:

I. INTRODUCTION

1. I am the Chief Information Officer (CIO) at Workday, a position I have held since March 2023. Prior to being the CIO of Workday, I was the CIO of Cloud Software Group from November 2022 to February 2023, and the CIO of TIBCO Software Inc. from November 2020 to October 2022. Prior to those roles I was the CIO of SolarWinds (the "Company"), a position I held from February 2017 until October 2020. I make this declaration in support of the motion for summary judgment of Defendants SolarWinds and Tim Brown (collectively, "Defendants"). The facts set forth herein are based on my personal knowledge and recollection and my review of certain SolarWinds records. If called upon to do so, I can and will competently testify to these facts.

2. As the CIO of SolarWinds, I was responsible for SolarWinds' information-technology ("IT") operations. Mr. Brown reported to me, and I reported to the Chief Technology Officer (CTO), Joseph Kim.

3. I understand that the Securities and Exchange Commission (SEC) relies on certain documents and emails that I drafted, reviewed, and/or received during my tenure at the Company. I submit this declaration to explain my understanding of those documents.

II. DOCUMENTS CITED BY THE SEC

A. Documents Concerning the Company's Efforts to Automate and Centralize Its Access-Provisioning Processes

4. I understand the SEC has cited a slide deck from January 2018 titled "User Access Management," Ex. A, and several NIST Scorecards and Quarterly Risk Reviews ("QRRs") containing notations about access controls, Exs. B, D-F. The portions of those documents that I understand the SEC has pointed to are about a long-term project during the Relevant Period to improve automation and centralization of the Company's access-provisioning processes.

5. Throughout my tenure at SolarWinds, the Company had role-based access controls in place. Specifically, we had what we called the "SARF process." Under that process, when an employee was onboarded at SolarWinds, a form would be filled out—called a "System Access Review Form" or "SARF"—that would specify the user's role. The form would then be provided to the Company's IT help desk, who would work to provision the employee with access based on the employee's role as indicated on the SARF. Specifically, the employee would receive a standard set of access rights designated for an employee in that role, as well as any additional access rights the SARF indicated the employee needed, as approved by an appropriate supervisor or system owner. The Company would follow a similar process whenever an employee changed

roles within the Company: a SARF form would be filled out that identified the employee's new role and any non-standard access rights they needed, and the IT help desk would work to change the employee's access rights based on the form. And when an employee was terminated, a reverse process would be followed: the IT help desk would receive notice of the employee's termination, and it would work to deprovision all of the access rights the employee had previously been assigned.

6. During my tenure at SolarWinds, we had various projects in place to improve the Company's access controls. In particular, as of 2018, the process the IT help desk would follow to implement access rights at a technical level was relatively manual and labor-intensive. When help desk staff would receive a SARF to implement, they would often need to separately configure access rights on a number of different systems in order to provision the employee with access to all the systems they needed (or, for an employee being terminated, to deprovision the employee's access to all the systems they had previously been using). This was particularly an issue given the growth of cloud-based software services around this time, which SolarWinds was increasingly using—such as Google Cloud. Access rights could not be configured on these cloud-based services using the standard version of Active Directory, a widely used Microsoft service that SolarWinds used at the time to manage its internal network.

7. The more systems that help desk staff needed to separately configure, the more chances there were for errors to be made in the provisioning and deprovisioning process. We would catch such errors from time to time in user access reviews that we regularly conducted during the Relevant Period, in which we would inventory user access rights on systems to confirm that they had been appropriately configured. These errors were not frequent. But as part of our efforts to continuously improve SolarWinds' cybersecurity controls, we wanted to

automate the access-provisioning process so that access rights could be configured as much as possible through a single centralized tool—thereby minimizing the number of systems that needed to be separately configured, and minimizing the chances for error.

8. We did this during the Relevant Period by migrating to a new identity and access management (IAM) service known as Microsoft Azure Active Directory ("Azure AD"). Azure AD was a relatively new product at the time, and it was specifically designed to provide a single, consolidated platform through which a company could manage access rights across many different types of applications. In particular, Azure AD came with what is known as single sign-on ("SSO") technology, which allows integration of third-party cloud services, like Google Cloud, so that user access rights on those services can be configured through Azure AD, as opposed to having to configure them separately on the third-party service.

9. This is what the January 2018 slide deck titled "User Access Management" is about—moving to a new technical tool to help us automate and centralize the access-provisioning process. *See* Ex. A (SW-SEC00043620) at -620. This can be seen, for example, from the subtitle on the title page: "Tool Evaluation & Recommendation." Ex. A at -620. Likewise, the third and fourth pages contain a "Tool Analysis" and "Solution Evaluation Summary," discussing the pros and cons of various tools we were considering in this regard, supported by an appendix with more details about each tool under consideration. Ex. A at -622-23. Finally, page 5 identifies the "Proposed Recommendation," which was to "[l]everage Azure [AD] for user access management," including because it "enables Single Sign On (SSO) and is pre-integrated with custom and commercial applications." Ex. A at -624.

10. I understand the SEC has quoted language in the "Problem Statement" on page 2 of the slide deck, stating: "Currently there is a collection of people who have access to many

systems and many people involved in provisioning access" and "The lack of standardized user access management processes that captures user provisioning (hiring), user changes (transfer) and user de-provisioning (resignation and termination), across the organization create a loss risk of organizational assets and personal data." *See* Ex. A at -621. To the extent the SEC is interpreting this language to mean that SolarWinds generally lacked role-based access controls, or that it lacked a process for provisioning users with access rights that was standardized in any way, that is not what the language meant. The SARF process was in place at the time of this slide deck, and it was a standard, but manual, process the Company followed for provisioning users with access. The slide deck was talking about standardization *at the technical level*—that is, a single tool that help desk staff could use to configure access rights across all applications at the company. The idea was that, with many help desk staff involved in provisioning user access, and many systems they sometimes had to configure (when users needed access to many different systems as part of their role), manual configuration of these systems created the potential for error, and thereby the potential for data loss. We were looking to minimize this risk by moving to a tool like Azure AD.

11. SolarWinds' migration to Azure AD is also the context for the excerpts I understand the SEC has cited from the NIST Scorecards and QRRs at issue. Specifically, I understand the SEC has cited a bullet at the top of a NIST Scorecard in a QRR presentation from August 2019 that states: "Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures." Ex. B (SW-SEC0001497) at -507. And I understand the SEC also cites to the fact that this NIST Scorecard lists a "1" as the score for "Authentication, Authorization and Identity Management." Ex. B at -507.

12. Tim Brown and I would put these NIST Scorecards together to include in our quarterly presentations to management (QRRs). They were intended to provide a quick snapshot of what the Company's cybersecurity program was doing in various areas, and in particular to highlight areas where we saw opportunities for improvement, so that we could get management's buy-in for the work and resources needed to pursue those opportunities. Tim and I would decide the scores in a relatively subjective fashion, by assigning higher scores to those areas where we felt the Company's controls were as mature as we wanted them to be, while assigning lower scores to areas where we wanted to mature our controls and that were the focus of planned or ongoing improvement efforts.

13. I helped put together the August 2019 NIST Scorecard the SEC cites, and I know that the excerpts it points to were about the Company's ongoing efforts at this time to centralize and automate its access control tooling, including in particular the migration to Azure AD. The Azure AD migration was a complex, long-term project we pursued across the Relevant Period. Shifting to a new IAM platform like Azure AD is a major organizational change that necessarily takes a long time to implement at any large corporation, as it basically involves rewiring configuration of access controls across the company. Many applications have to be integrated with the new platform, and each integration needs to be rolled out and tested carefully to prevent glitches that could disrupt company operations or result in erroneous user access configurations.

14. The August 2019 NIST Scorecard at issue was simply highlighting the need for this ongoing project. The bullet about "[a]ccess and privilege to critical systems / data" being "inappropriate" was a shorthand reference to access being managed in a way that was decentralized at a technical level—which created the risk of error, as discussed above. Again, we wanted to minimize this risk through migrating to centralized, automated tooling like Azure AD.

This is reflected in another bullet on the slide stating: "Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets." Ex. B at -507. That was the main step the Company was taking at this time to "improve" our "internal processes | procedures"—ensuring that access rights on all critical systems were centrally managed through Azure AD.[1]

15. This is also what the "1" score on the slide was a reference to. A common way that companies mature their controls under the NIST CSF is by automating and centralizing them, so that they are executed in a technologically consistent way across the organization. That is what we were seeking to do with access management by migrating to Azure AD. While the project was still ongoing—which it was as of August 2019—we scored the Identity and Access Management category on our NIST Scorecards as a "1," to convey to management that this was an important opportunity for improvement but that it was still in progress. This is reflected, for example, in a draft of this same slide, which identifies the "KPI" (key performance indicator) driving this score as the "[n]umber of assets (mission/business critical) with AD Authentication enabled vs. not enabled)"—*i.e.*, the number of systems that had been integrated with Azure AD to date as part of this project. Ex. C (SW-SEC00623600) at -609.

16. The ongoing rollout of Azure AD is also what is referred to in notations the SEC cites from subsequent QRR presentations, including: a note from a November 2019 QRR presentation stating "Pushing forward with AD authentication guidelines for critical mission systems." Ex. D (SW-SEC00001551) at -552; and notes from a March 2020 QRR presentation

[1] We were also pursuing implementation of a centralized privileged access management ("PAM") tool, known as "Thycotic," that would allow us to manage storage of highly privileged credentials across the Company in a technically uniform manner. This, too, was part of the efforts we were making to improve our access management processes at the time, which we would have discussed with management as part of this presentation.

and May 2020 QRR presentation referencing enforcement of "AD authentication" among improvements being made, Ex. E (SW-SEC00001608) at -611 & Ex. F (SW-SEC00001602) at 605. Mr. Brown and I were simply keeping management informed of our continuing progress in implementing this extensive project.

17. The notes in the slides were not intended for an external audience, nor were they intended to stand on their own, without any explanation from myself or Mr. Brown.

18. None of these notes say or were intended to convey that SolarWinds lacked role-based access controls.

B. "Preliminary Assessment" of Effort Required to Meet FedRAMP Controls

19. I understand the SEC has cited a "preliminary assessment" that I asked an employee under me, Kellie Pierce, to prepare, relating to certification under the Federal Risk and Authorization Management Program, known as "FedRAMP."

20. In 2019, the sales team within SolarWinds' cloud software business line—which had recently been acquired by the Company—wanted to be able to sell its products to the federal government. In order for the federal government to purchase cloud software, however, the software must be certified under FedRAMP. FedRAMP certification requires meeting a highly demanding set of controls, as established through extensive documentation validated by a third-party auditor. Obtaining FedRAMP certification would have been a very expensive and time consuming project for the Company to undertake. I did not believe that the result—being able to sell the federal government our cloud products, which involved only a very small portion of SolarWinds' overall business—would be worth the effort involved.

21. In order to come up with a rough measure of the effort that would be involved, I asked Ms. Pierce to conduct a preliminary review of what it would take to obtain FedRAMP certification. Ms. Pierce was not a FedRAMP expert.

22. What Ms. Pierce did was merely an internal budget exercise designed to provide a starting point for discussions within the Company about whether to pursue FedRAMP certification, and was not intended, in my view, to be an accurate record of whether the Company had the controls required by FedRAMP in place. This is reflected, in my view, in Ms. Pierce's correspondence with the Cloud team about the preliminary assessment, in which she stated that her "takeaway" was that achieving FedRAMP compliance would take a "moderate to significant level of effort" from various SolarWinds teams, and asked the Cloud business line to prepare a budget request and business justification for the resources that would be required. *See* Ex. G (SW-SEC00045356) at -356-57. SolarWinds never ended up pursuing FedRAMP certification during my tenure at the Company, as the required investment was not deemed worth it.

C. Remark in QRR About User Access Reviews That Needed to Be Re-Run

23. I understand the SEC is citing a note in a NIST Scorecard included in a QRR presentation from March 2020, stating in a row in a chart, under a column titled "Key Risks": "Significant deficiencies in user access management." Ex. E at -611.

24. I specifically remember what the notation "Significant deficiencies in user access management" in this chart referred to: In preparing for our 2020 SOX audit, we needed to have user access reviews that we could show our SOX auditors for systems within the scope of the audit. Our internal audit team discovered that the individual who led the effort to prepare these reviews requested data from the wrong window of time, resulting in a significant number of users being excluded from the review who should have been included. This required all of the reviews to be redone—which I found frustrating and wanted to note to management in this QRR presentation. However, the problem was fixed in time for the external SOX audit and did not result in any deficiency finding from our external auditor. It was merely an *internally* discovered SOX deficiency that I was noting—and one that we promptly fixed before our actual SOX audit.

25. I understand that the SEC has also cited a QRR presentation from May 2020 that included this same notation—"Significant deficiencies in user access management. *See* Ex. F at 605. The only reason a later presentation would contain the same notation is that we did not start from scratch in preparing each QRR presentation, and it was common for a notation made in one presentation to be carried over to another, especially if they were presentations within the same year. The notation at issue refers to the same thing in the May 2020 presentation—the deficiencies in the user access reviews that were initially prepared for our SOX audit for 2020, which we fixed before the completion of the external audit.

III. CONCLUSION

26. I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 4/25/2025

Rani Johnson